



---

# A PI=5 CONTROLLED INTERFACE FOR FILE TRANSFER

Paul D. Sands  
[pdsands@sandia.gov](mailto:pdsands@sandia.gov)


Sandia is a multiprogram laboratory operated by Sandia Corporation,  
a Lockheed Martin Company, for the United States Department of Energy  
under Contract DE-AC04-94AL85000.



# An MLS FTP Guard

---

- The Need for an FTP Guard
- Why Use Evaluated Products?
- The Basic Design
- Phased Approach
- What's Happened
- What's Next



## The Need: Access from Classified Systems to Unclassified Data

---

- Much of the data used in the weapons program is unclassified (e.g., drawings of commercial parts)
- This data needs to be in the unclassified environment
  - ◆ for interchange with suppliers
  - ◆ to avoid the high costs of classified computing
- Dual copies must be maintained in the classified environment, where weapons design occurs
  - ◆ Data is moved via off-line media
  - ◆ Dual copies get out of synch



# The Need for An FTP Guard

---

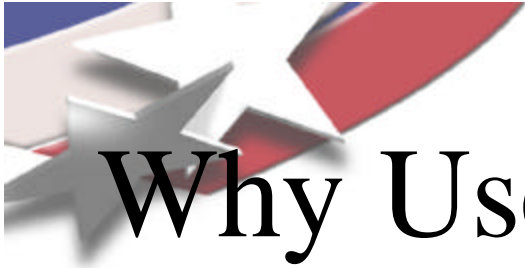
- Classified Designs use Many Unclassified Components
- Some of the Choices
  - ◆ Duplicate the Files
    - Synchronization Problems
  - ◆ Keep them in the Unclassified Network
    - Off-line Transfer or Electronic Connection



## The Solution: Electronic Access from Classified Systems to Unclassified Data

---

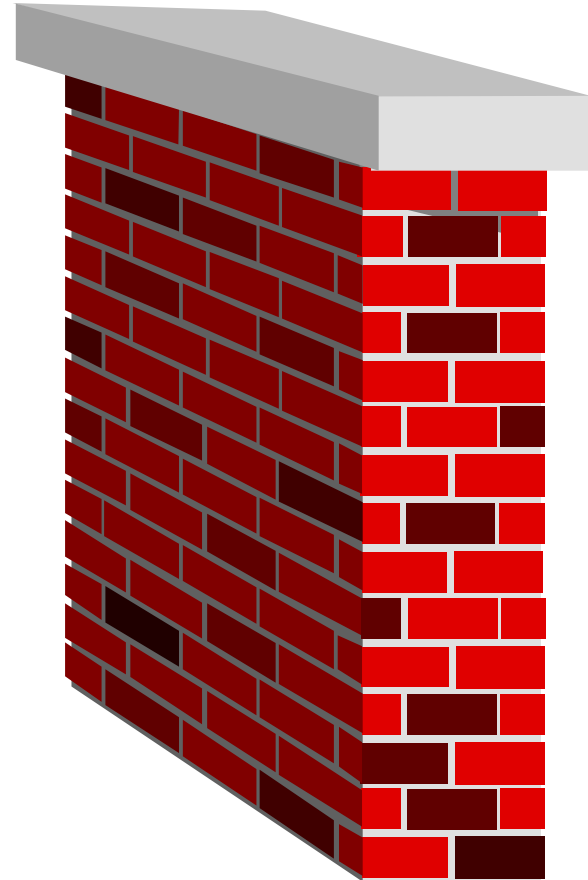
- Allows master copy to be maintained in the unclassified environment
- Files can be easily moved to synchronize classified copies with unclassified master



# Why Use Evaluated Products?

---

- Known Quality
  - ◆ Evaluated & Tested
  - ◆ Security from the Initial Design
- Standard Methods
- Gives Known Result
  - ◆ Start with B3
  - ◆ End with B3
- Downside: later

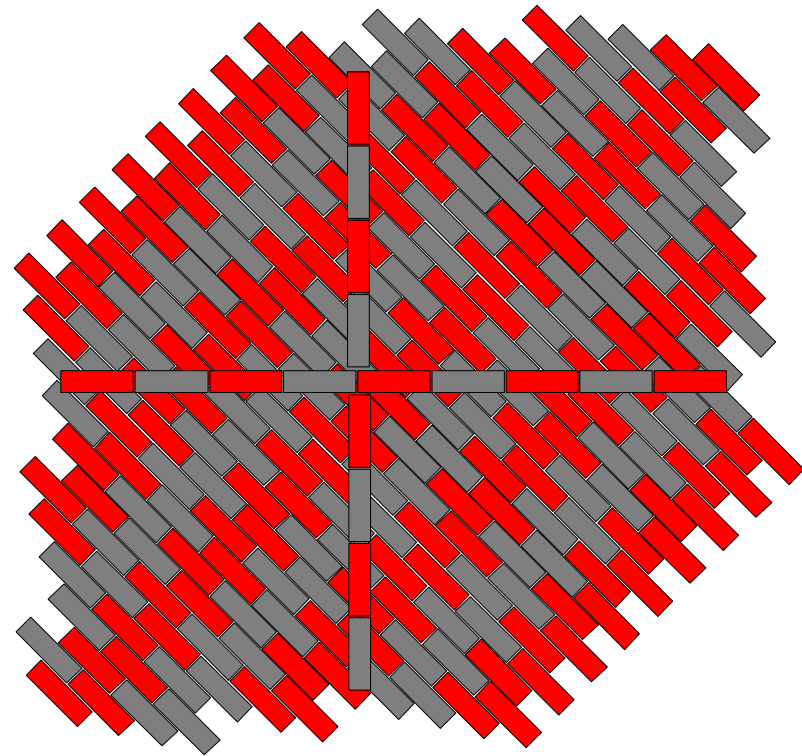




# Do Your Own Thing

---

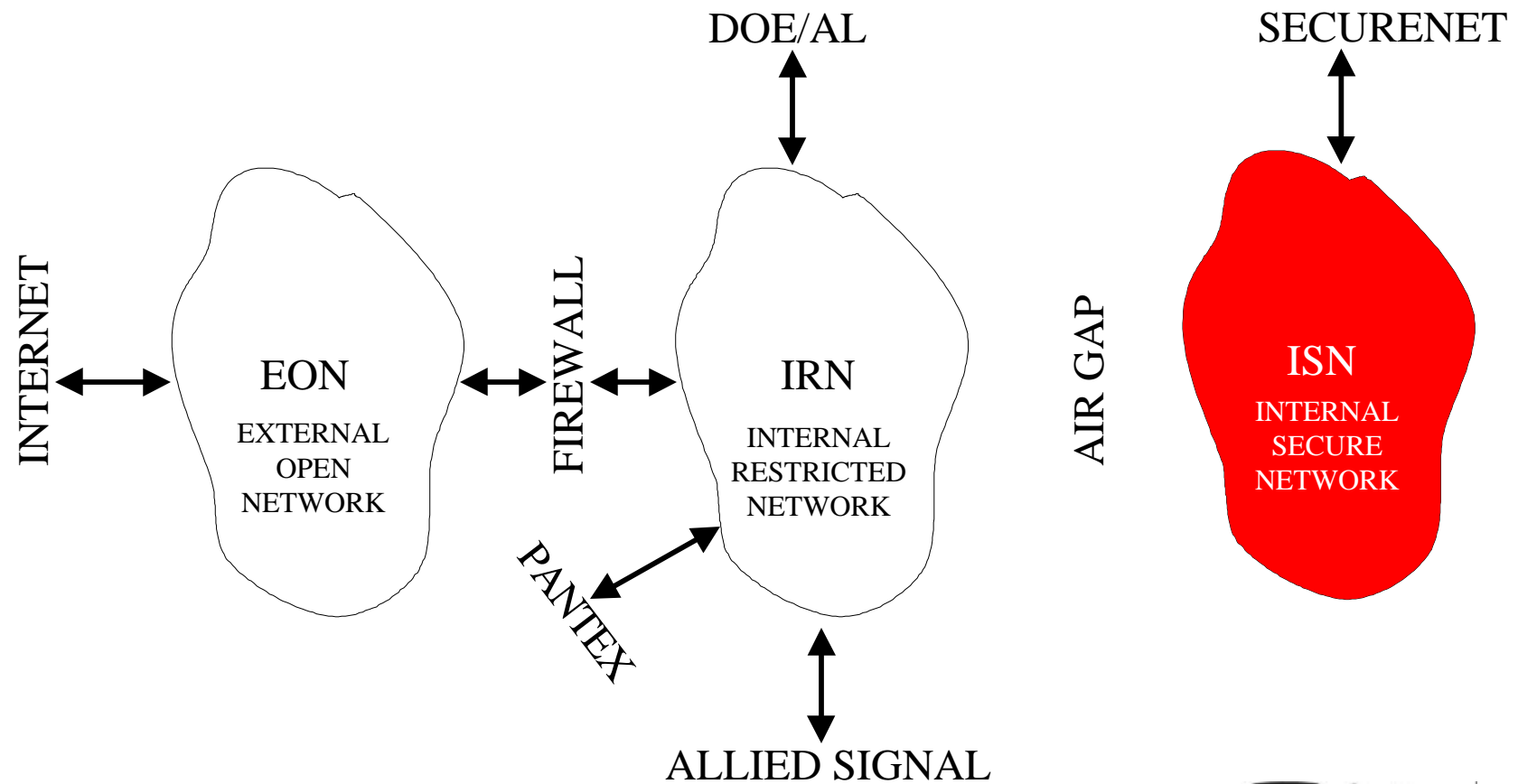
- Unknown Quality
  - ◆ Might be Better
  - ◆ Might be Windows95
- Difficult for DAA to Evaluate
- Should be Subjected to NCSC-like Review





# The Starting Point

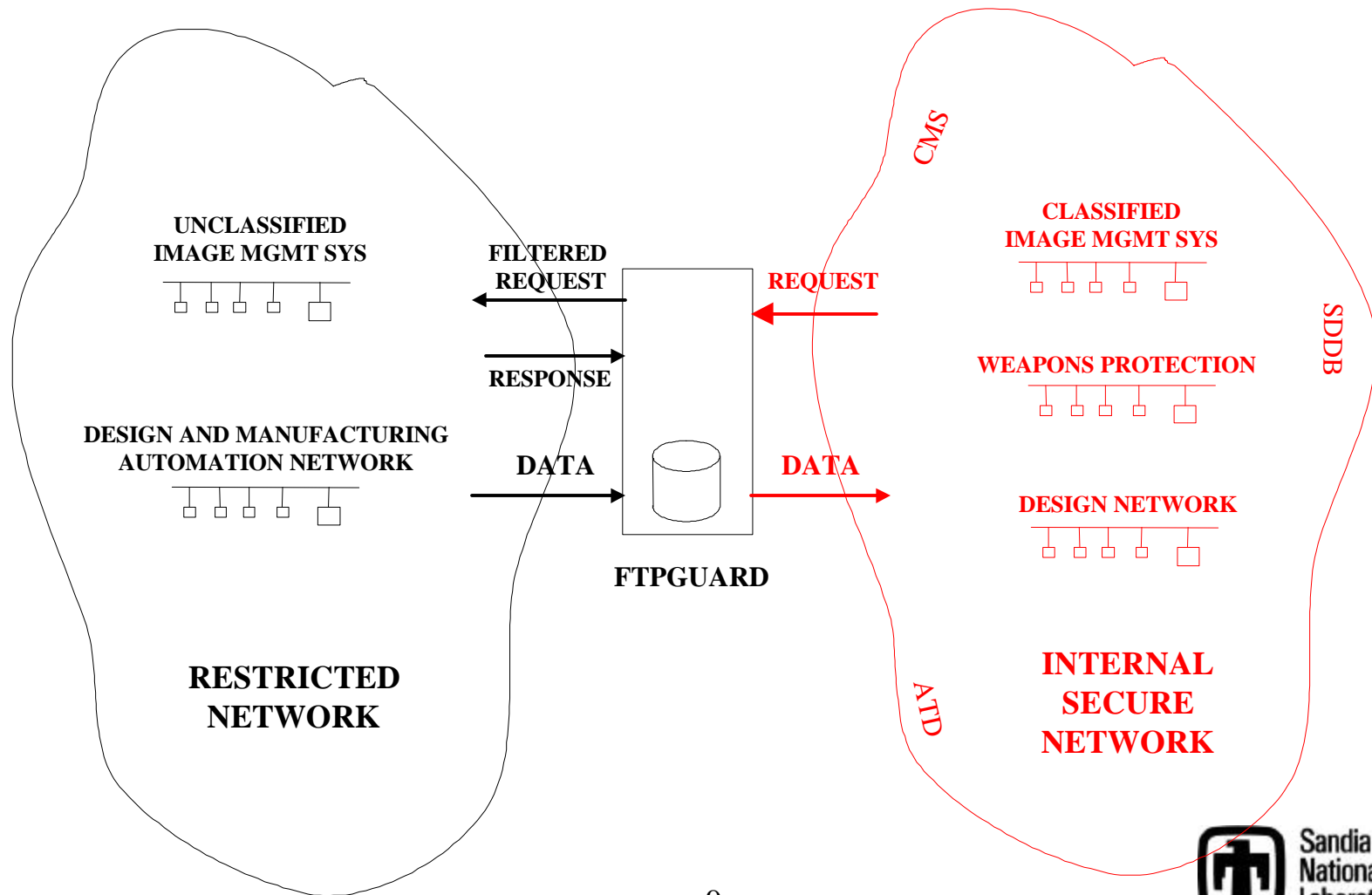
---

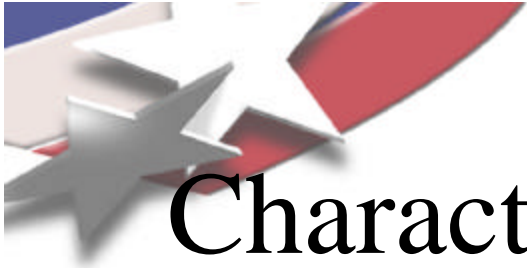






# The Destination

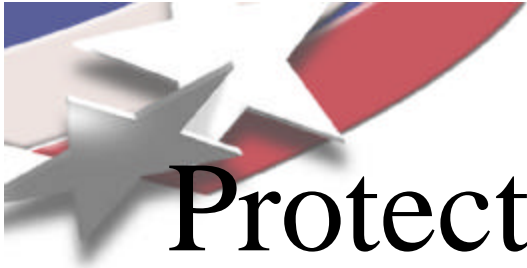




# Characteristics of the Guard

---

- Works with Standard, Unmodified FTP Client from a Classified (ISN) System
- To the Classified User, it Looks Like they are Talking to the Unclassified Server (They never really are)
- No Action on the Classified Side Causes a Visible Effect on the Unclassified Side (No Covert Channel)



# Protection Index = 5

---

- Most Sensitive Info (High Network) is SRD
- Least Cleared User (of Low Network) is Uncleared
- Some of the Requirements
  - ◆ B3, Auditing, Active Monitoring
  - ◆ IV&V, Life Cycle Assurances
  - ◆ Confidence in Software Sources
  - ◆ Separation of Duties

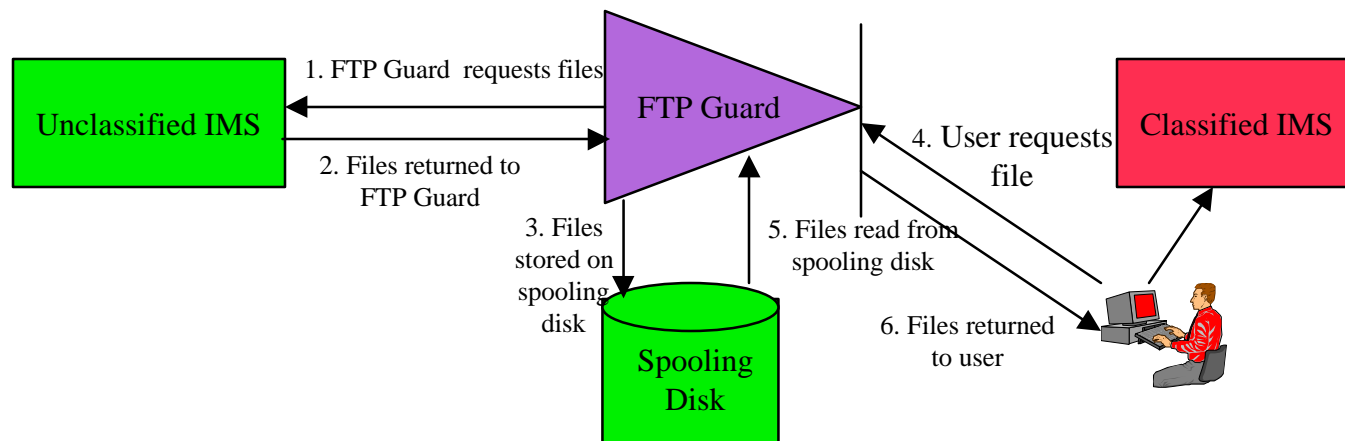


# Phase I: Automated Xfer

---

- Time-Driven Job on Guard (cronjob)  
Causes IRN Files to be Spooled to the Guard
- ISN FTP Client Gets Files
- No privileged processes: Every process is bound by the usual rules
  - ◆ No read up
  - ◆ No write down

# Phase I: Periodic Staging of Selected Files

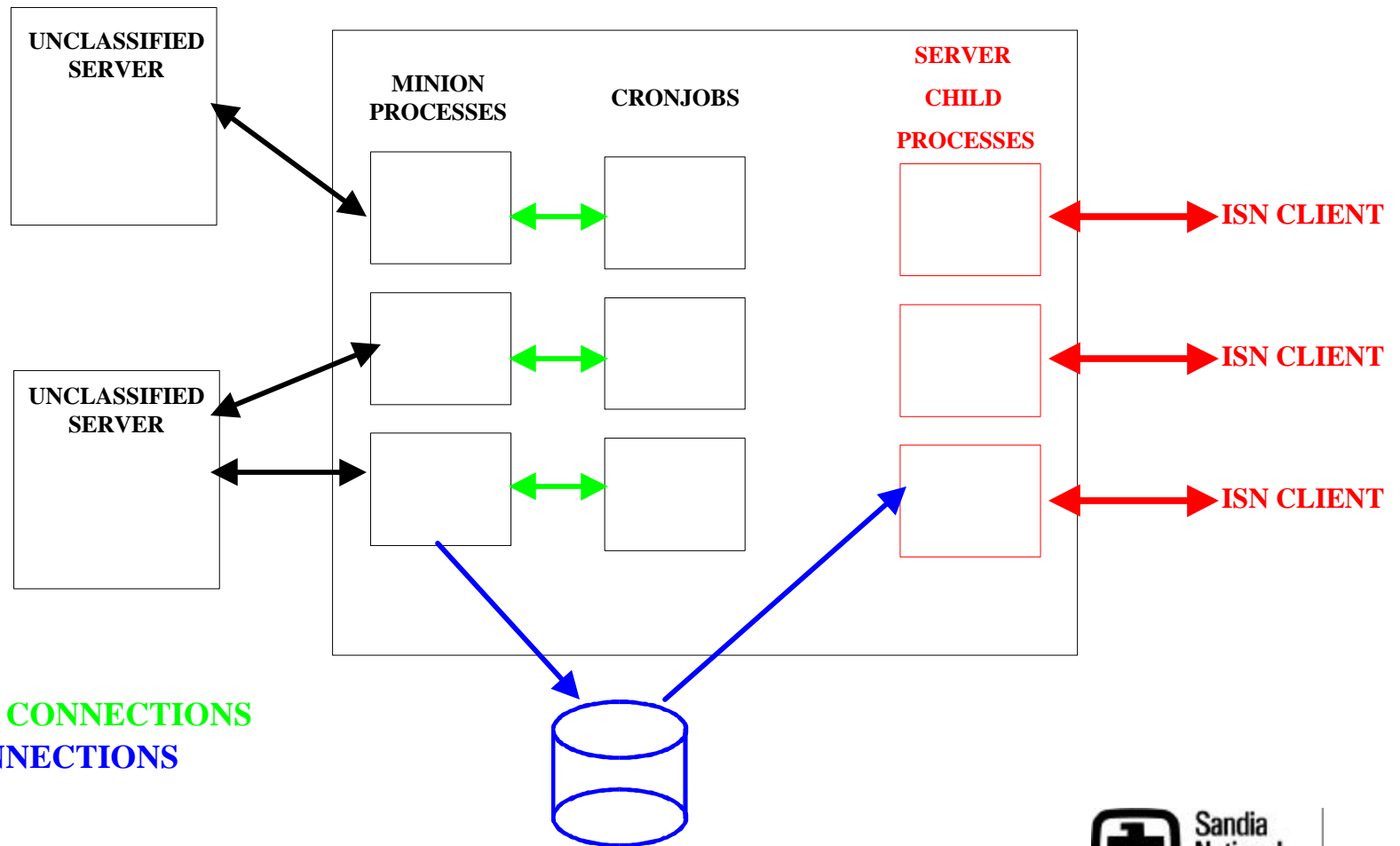


Phase 1: Files must be staged from unclassified system to FTP Guard spooling disk (by prior arrangement) before becoming accessible to classified user.

Note: Bandwidth is limited by size of the spooling disk



# Phase I Processes



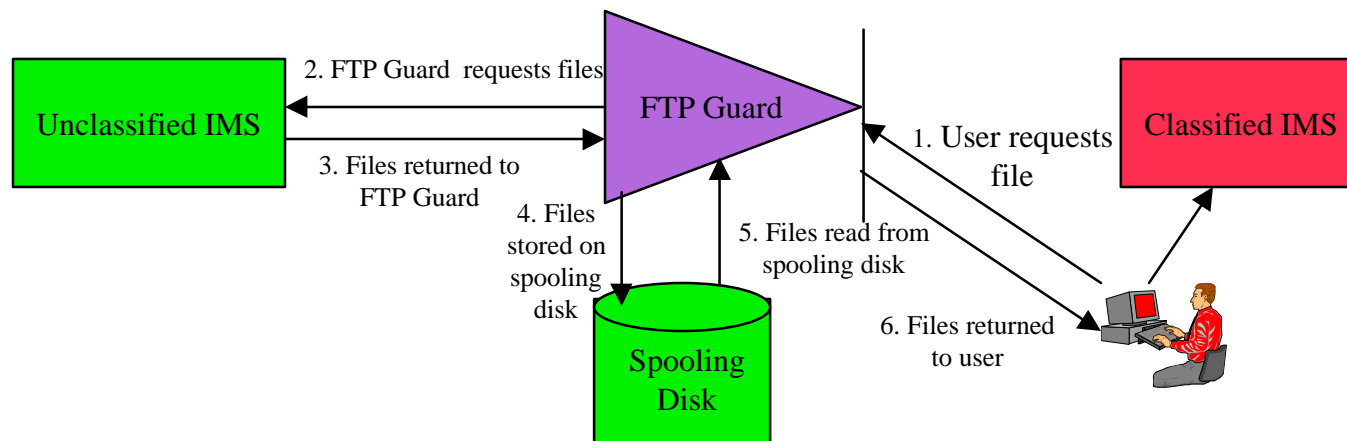


## Phase II: Directed Xfer

---

- Everything in Phase I plus
- Classified Users with SecurID Cards can Ask for Unspooled Data
- A High-Side Process must be allowed to Send Messages to a Low-Side Process
- Only Unclassified Information is Contained in Requests
  - ◆ How do we know? later

## Phase II: Access to Files On Demand



Phase 2: Files staged from unclassified system to FTP Guard spooling disk and returned to classified user on demand.

Phase 3: Web Access will be similar to Phase 2, except the HTTP protocol will be used.



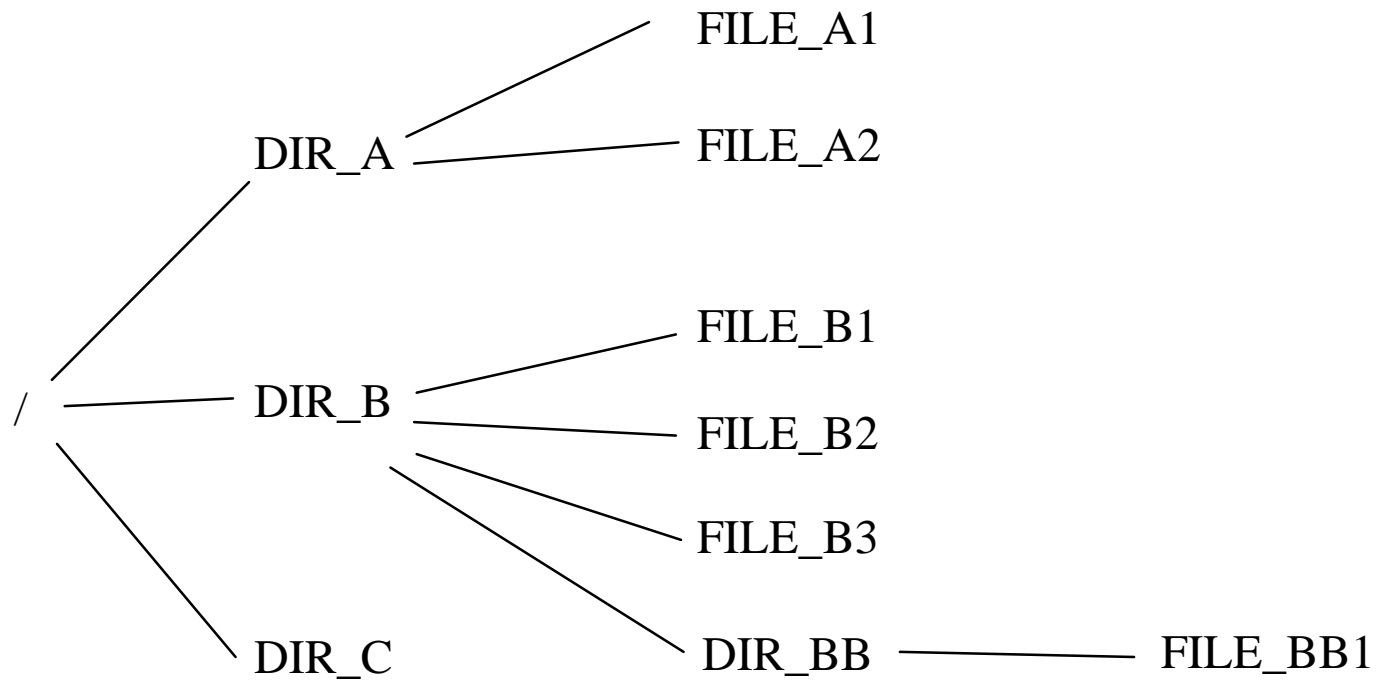


# No Classified Data Goes Out

---

- High Processes Make Choices from Unclassified Objects
- No Process Sends an Arbitrary String from the Classified to the Unclassified Side
- Unclassified Data Moves to the Classified Side, but Only by Request (from the Classified Side)

FILE SYSTEM ON REMOTE (BLACK) SYSTEM SHOWN BELOW.  
{NOT YET VISIBLE TO RED USER}

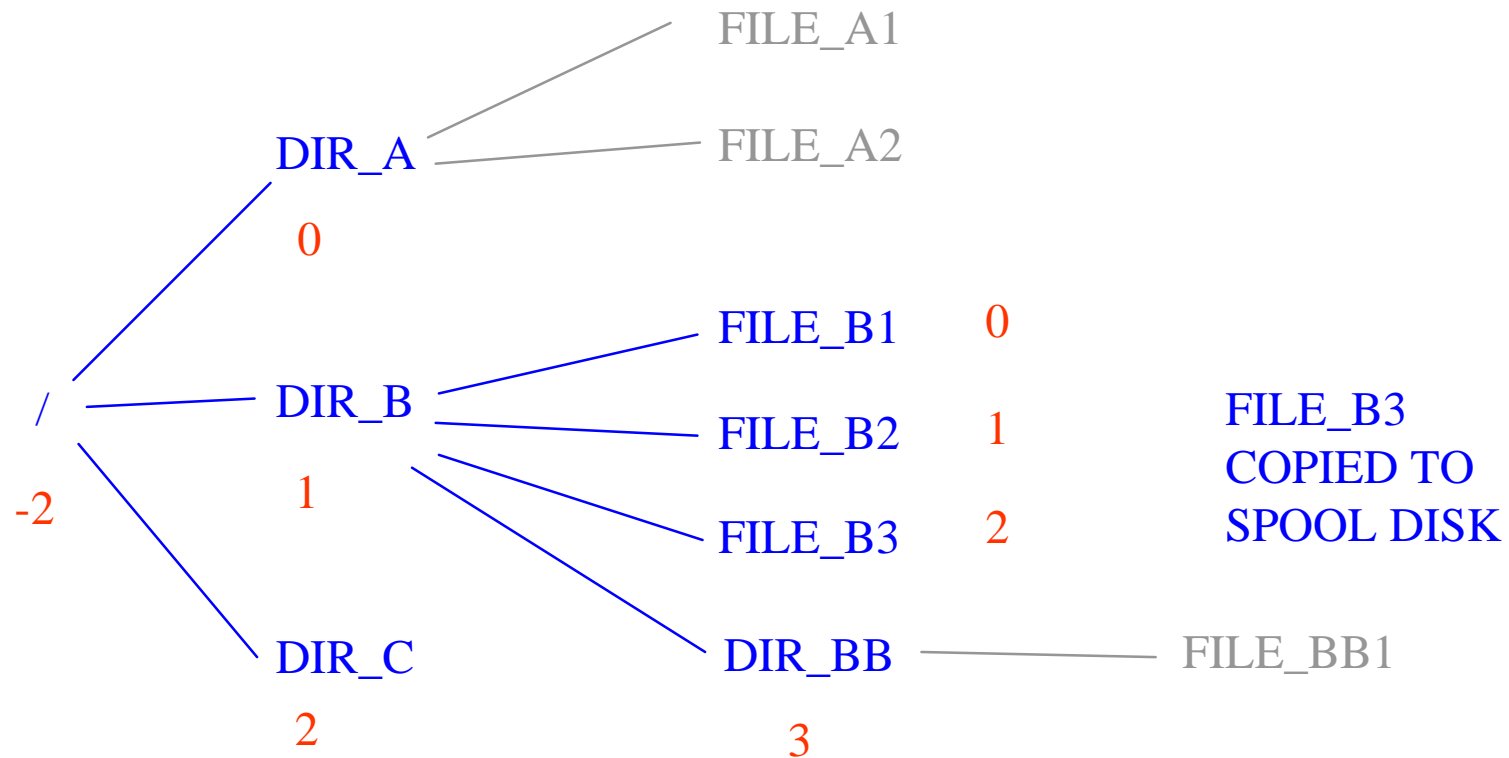


USER COMMAND: GET /DIR\_B/FILE\_B3

COMMAND SENT: CD -2 {CHANGE TO ROOT & LIST}

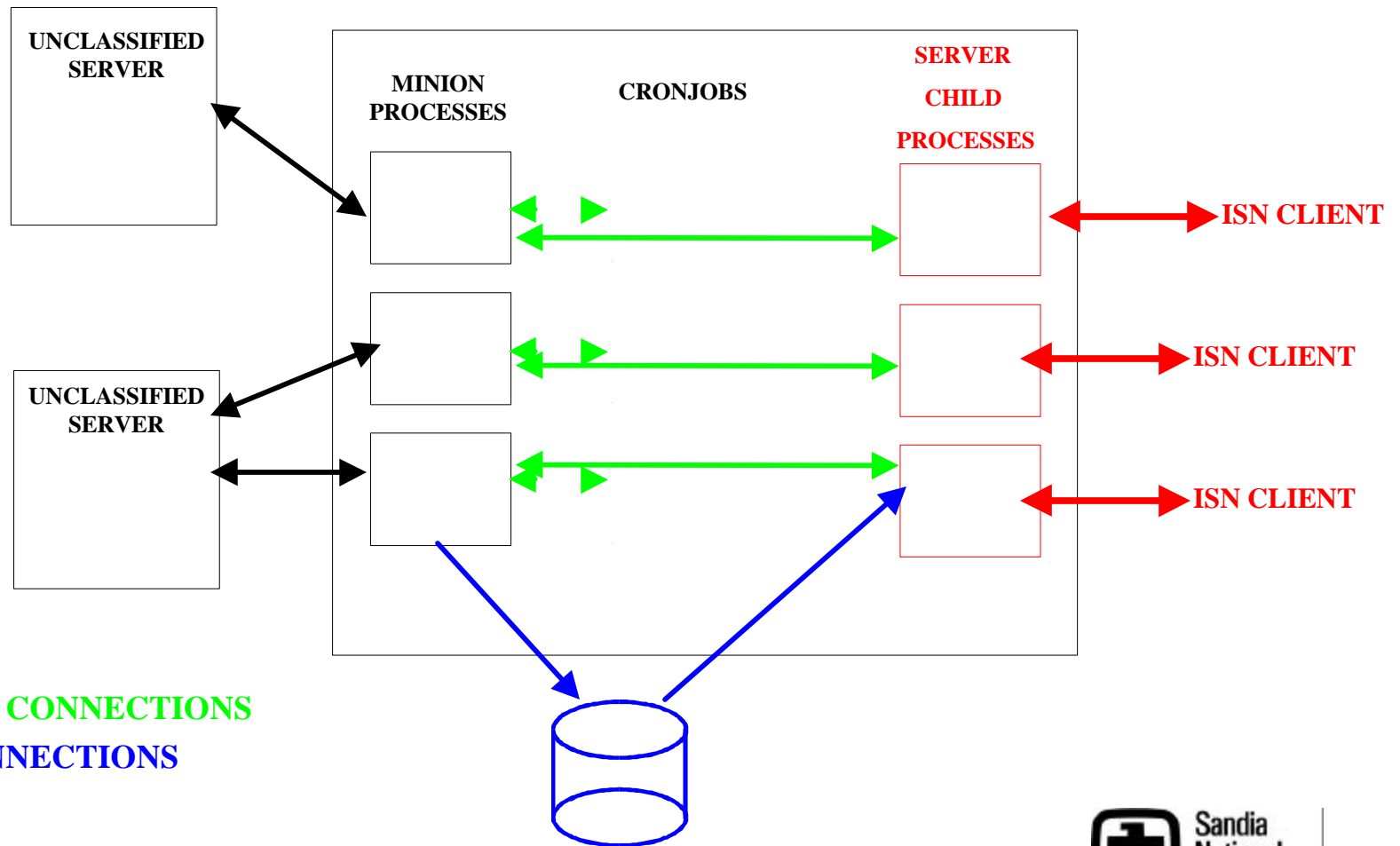
CD 1 {CHANGE TO DIR\_B & LIST}

GET 2 {GET FILE\_B3}





# Phase II Processes

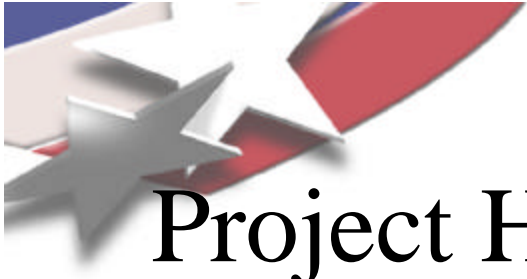




# Possible Phase III

---

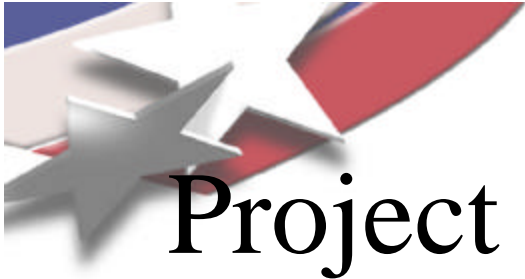
- WWW Proxy Server between Red and Black
  - ◆ Guard Begins with a List of Valid URLs (e.g., Certain Home Pages)
  - ◆ Any URL on a Page Fetched by a User is Added to the List for that User
  - ◆ Since the Only strings that can be Sent Out have come from Unclassified Sources, no Chance of Accidentally Sending Classified Info
  - ◆ Requires filtering of incoming files to eliminate executable content (e.g., Java, Postscript)



# Project History

---

- Project begun - 10/96
- Conceptual design complete and presented to DOE - 12/96
- First security plan submitted to DOE - 2/97
- IV&V of FTP Guard Design - 6/97
- IV&V Report recommends approval - 7/97
- DOE approves security plan - 9/97
- Security test plan submitted to DOE - 10/97
- DOE approves security test plan - 11/97
- Security tests conducted and results documented - 12/97
- DOE accredits FTP Guard for 60 days - 12/97
- DOE withholds accreditation pending NSA eval. - 2/98



# Project Status

---

## ■ Phase I

- ◆ Programming Complete
- ◆ IV&V Favorable, Security and Test Plans Approved
- ◆ Tests conducted in November/December
- ◆ Interim accreditation Dec 97 to Feb 98
- ◆ DOE decided to wait for final NCSC report on XTS-300

## ■ Phase II

- ◆ Programming to finish Sep 30, 1998
- ◆ Second IV&V Needed
- ◆ Cannot predict when DOE will accredit



# Future Milestones

---

- XTS-300 Operating System successfully completes RAMP evaluation by NSA for current release - 04/98
- Implement Phase I changes requested by IV&V and receive final accreditation - 04/98
- Phase II Software Complete - 09/98
- Phase II IV&V Complete - 10/98
- Phase II Accredited and Operational - 01/99
- Phase III Preliminary Design Complete - 03/99
- Detailed Design updated for Phase III - 06/99
- Phase III Implementation Complete - 12/99
- Phase III IV&V Completed successfully - 01/00
- Phase III (Web Access) Accredited - 04/00





# Difficulty of Listed Products

---

- By the time any product is fully approved, it is obsolete
  - ◆ SCOMP based on PDP-11 achieved A1 in December 1984
  - ◆ Ran at less than 10% of current VAX model
  - ◆ Current B3 Wang XTS-300 runs on 486
  - ◆ Pentium 166 to be approved shortly
- DAAs may be willing to accept products in RAMP
  - ◆ These are based on approved products
  - ◆ Security model, etc. is the same
  - ◆ Significant testing and review has already been done
- If RAMP is not considered superior to untested, developers will try to use less secure products